BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

Infrastructure of Multi-Application Smart Card

(in the concerns of access control)

CHAN, Siu-cheung Charles

1. Introduction

The smart card is a credit card sized plastic card embedded with an integrated circuit chip which provides memory storage and processing power. Nowadays, through the new and upcoming technologies, the size and ability of the smart card continue to increase. 4K or 8K byte cards are no longer new. The latest smart card which make uses of optical technology even provides up to several mega-bytes storage spaces.

Besides the capacity, the micro chip on the smart card allows the implementation of cryptographic and authentication algorithms, so that information stored on it can be secured and protected. Therefore off-line transactions are possible while the magnetic stripe card requires on-line database verification. As a result, many companies are going to develop or enhance their services by using the smart card as it provides more storage space and offers more security and confidentiality when compared with the traditional magnetic stripe card.

An important issue in the smart card industry is the capability of the smart card, which makes the integration of multiple applications into a single smart card feasible. In the concerns of access control, this paper discusses different infrastructure of multiple application smart card, and tries to develop both procedural and technical mechanisms to implement such a system in the terms of data ownership and management, data directory configuration and partitioning, security and data sharing, and system application expansion, etc.

2. Multiple Application Smart Card Systems

Most of the smart card systems in use today serve one purpose and are related to just one process. For example, the smart telephone card which makes public telephones convenient, electronic money which replaces coins and bank notes, the medical card which stores medical history and insurance information, and the electronic identification card which control access to data and facilities, etc. All of these applications are stored in different smart card systems separately, and lead to the same situation and problem as with the traditional magnetic stripe card system which require users to carry multiple cards for multiple applications.

In fact, as mentioned above, the smart card has the capability to integrate those applications together to form a multiple application card by utilising its embedded microprocessor and memory storage spaces.

However, this kind of integration is always limited by some of the external logical elements rather than technical issues. For instance, in single application card system, data stored in the card or even the card itself always belongs to the card issuer. In the case of more than one application residing in a single card, this becomes impractical.

Moreover, we also have to consider how to partition the memory spaces for different applications, and manage the rights and privileges of data accessing. This also relates to data directory configuration and securities between each of them. Furthermore, the ability for applications to communicate or share data between each others is another important concern which may affect the whole design of the system and its operability.

Therefore, based on the natures and purposes of different applications, we discuss three different kinds of infrastructure of multiple application smart card systems. The first one is minor applications which co-operate with a dominant application. The second one will be the integration of multiple applications under a single specification. At last, multiple independent applications installed on a single card will be taken into an account.

---

3. Minor Applications Co-operate With Dominant Application

While most of the existing smart card applications do not fully utilise both of the memory storage and processing power of the card, it is feasible to integrate other minor applications which make use of the existing resources and functionalities of the dominant system together. This kind of system always requires co-operation between application providers. Figure 1 shows an overview of this system.

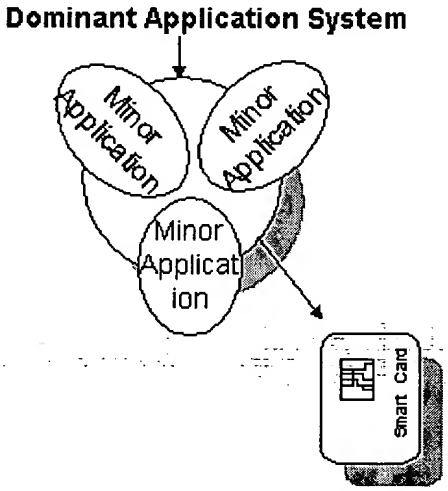

Figure 1: Minor applications co-operate with dominant Application

3.1 Data Ownership and Management

Ownership and management of data can be made under the corresponding co-operative contracts and schemes. However, in most of the cases, management of minor applications will fall on the dominant application as they rely on the existing system resources such as cryptographic algorithm and

authentication processing. In addition, minor applications may need to make use of part of the dominant application to perform their jobs, consequently all of the applications under this kind of integration have to be considered as a whole system and managed together in order to achieve and provide multiple functions and services. Distribution of the card can be made under the co-operation plans or marketing strategies which depends on whether minor applications come with the dominant application or minor applications are acted as an upgrade of services.

3.2 Data Directory Configuration and Partitioning

As the minor applications reside under the existing dominant application and co-operate with it, they should be acted as a subset under the dominant application logically. Figure 2 below shows the logical view and relationship between applications.

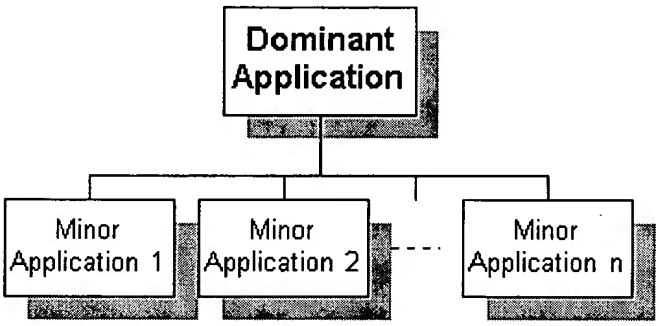

Figure 2: Logical view of applications in this model

Technically, this can be done by placing minor applications under different sub-directories or functional groups which are below the dominant application directory. Dedicated files (DFs) can be used to separate and organise applications. Figure 3 displays the structure and organisation of memory spaces inside the smart card.

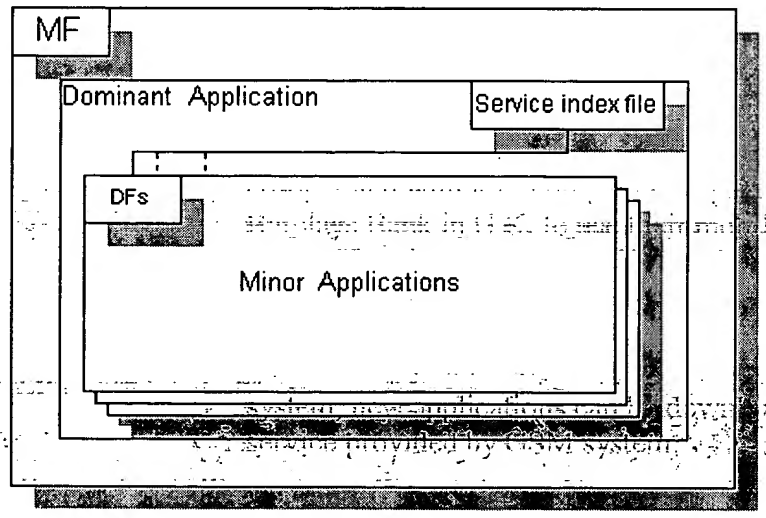

Figure 3: Structure and organisation inside the smart card

3.3 Security and Data Sharing

From the view of dominant application, minor applications are treated as trusted applications because

they are implemented according to the compromised co-operation plan, and this is why minor applications are allowed to make use of the dominant application system resources to perform their services. Therefore data communication between them should be regarded as safe and secure. However the relationships between each minor applications should be treated as untrusted entities. Hence transfer of data between minor and dominant application should be made under a exclusive channel in order to prevent wire tapping. The data sharing between minor applications should be accomplished by establishing another exclusive channels under another co-operative scheme.

3.4 Application Invocation and Authentication

Minor applications should be invoked by the dominant application as they are a subset of it. A service index file which stores identification numbers or dedicated file Ids of available services should be implemented by the dominant application system. An only the dominant application system has the access right on it. An invocation algorithm between end-user, dominant and minor applications have to be provided as well, so that different applications can be executed when requested. Authentication of them should rely on the provided mechanism from the dominant application system as they co-operate with each others, therefore each application does not need to implement its own security algorithm. Nevertheless, an additional or second authentication can be done by individual applications when there is a need.

3.5 Application Expansion

Whenever there is a new application added to the card, that application must be implemented under a compromised co-operation program with the dominant application provider. From that program, service Id, dedicated file Id to be used, and the way to co-operate with each others can be determined without contradiction. Card holders can have the new application added through the particular authentication procedure which is designed for adding new applications.

3.6 Examples and Summary

According to *NewsPage from individual (May 97)*, Gemplus Corporation, one of the world's leading producers of smart cards, announced that its new GemXplore smart card is compatible with GSM Phase 2+ which is the latest phase of the GSM (Global System for Mobile Communications) telecommunications standard that supports multi-application development. The company also announced that it has completed the development of the first GSM phase 2+ compliant application which is co-operated with four companies to provide remote banking application that allows customers of Barclays Bank in U.K. to use their mobile phones to access account information through the phone's screen. The service also provide mini-statements which is similar to an ATM screen.

The integration between remote banking application and the dominant GSM application system shows a good example of multiple application smart card system as described above. Furthermore, under this system, new applications can be downloaded or updated over the air with the enhanced short message service provided by GSM system.

---

4. Multiple Applications Under Single Specification

In the present days, many card applications serve similar purposes or make use of similar resources to perform their services, such as different kinds of identification cards or licenses, different sort of

merchant incentive card which stores "points" for frequent purchaser programs, and credit/debit cards from different financial institutes, etc. These applications are suitable and feasible to integrate together in order to increase functionality of the card and decrease the resources spending by sharing common required information such as card holder's information. One of the conditions for applications to be united in this system is that they have to be governed by a single specification or standard under a certain authority. Figure 4 illustrates this model.

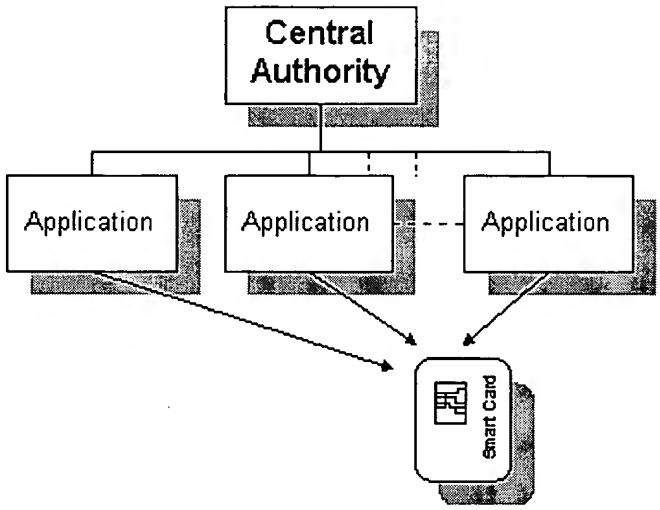

Figure 4: Multiple applications under single specification

4.1 Data Ownership and Management

Ownership and management of the card and data becomes a bit complicated because applications come from different institutes or organisations. However, as all the applications follow the same specification and standard from a certain authority, it is recommended to assign the corresponding authority to establish the system and distribute the card. The card can either belong to that authority or the end user can purchase it depending on the nature of services provided by those applications. Management of those applications should be made upon the request of the card holder when he or she can provide positive identification that he or she is the correct owner. On the other hand, when an organisation which establishes the card system provides applications for its own card, that particular organisation can have both of the ownership and management of the card.

4.2 Data Directory Configuration and Partitioning

Before implementing or providing a new application, application provider has to request an unique identification number from the corresponding authority, and that unique number may serves as a dedicated file (DF) number so that the new application can be stored under the assigned functional group without conflict with others. In addition, a particular identification number is reserved for the common criteria application which is developed by the central authority and will be installed during the issue of the card. That application is used to handle the common requirements of all the integrated applications such as user identification and information. Figure 5 shows a general view of the directory structure.

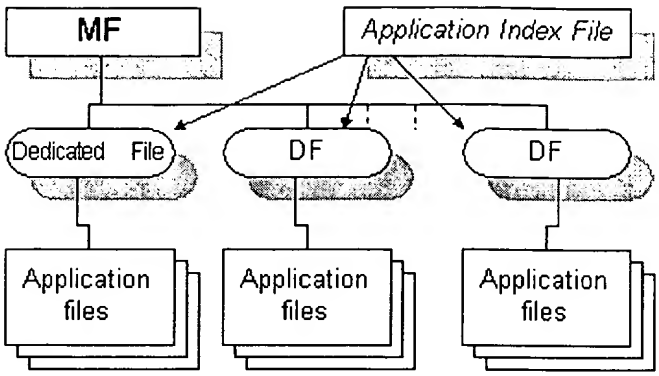

Figure 5: General view of directory structure

4.3 Security and Data Sharing

All the applications integrated into this system should provide and achieve similar services and functions, so that they will have similar requirements on the level of security. As a result, cryptographic and security mechanisms implemented by the central authority can be shared and used by different applications. Applications which are going to be united should agree and conform to the specification from the corresponding central authority.

However, accessing individual applications should be protected by the system security module. This can be done by identifying the source of request and the destinated application. For example, when application *A* is activated by the user, *A* will issue a request, with both of the source and destination of *A*, to the shared common security module for authentication. If it is positive, a ticket of accessing *A* will be returned to the source, it will be *A* in this example. When *A* received the ticket and discover the ticket of access is *A*, then it will unlock itself and allow for access. Figure 6 illustrates this mechanism.

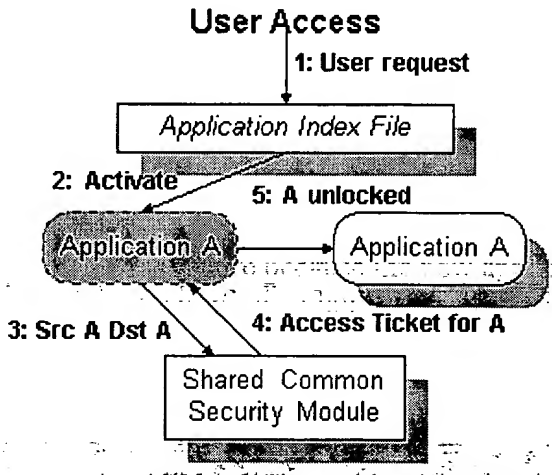

Figure 6: Authentication of an application

When there is a need of sharing data, applications involved should implement a second security module. For example, when application *A* request access of application *B*, *A* issues a request, with the source of *A* and destination of *B*, to the shared common security module. When the security module realises the source is different from the destination, it then pass the request to *B*. *B* will activate its own security module upon the receive of the request. After successful acknowledgment, *B* unlock itself for the access of *A*. All the rest of transactions and communications between applications should have the source and

destination specified in order to protect the access of correct applications. Figure 7 shows this model.

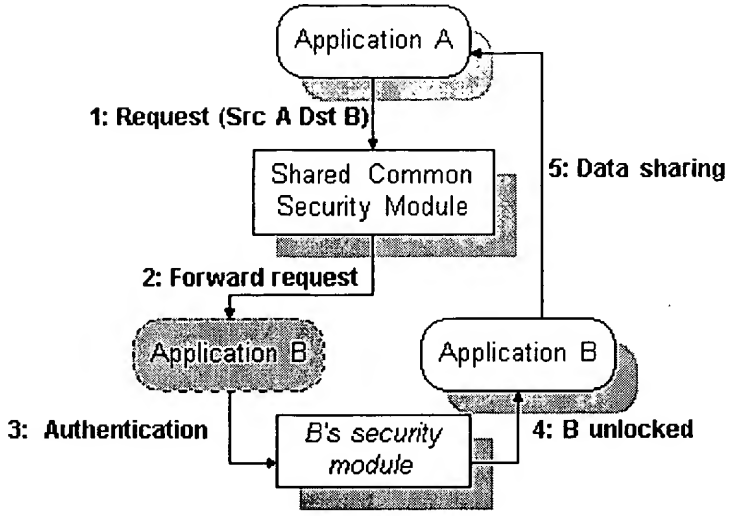

Figure 7: Data sharing between applications

4.4 Application Invocation and Authentication

A service index file, which contains information about the available applications and links to corresponding dedicated files, should be updated whenever there is a new application added. This file should be allowed to read by anyone, but writable by the central authority only. The user should invoke the application through the index file or invoke it directly in case when the dedicated file Id is known. The application should be activated and a request of authentication sent to the shared common security module with the source and destination as described above in section 4.3. Details are shown on figure 6. The way of authentication should follow the standard specification under the corresponding authority which may differ from each others.

4.5 Application Expansion

All the new applications which are going to be integrated should be registered to the respective authority in order to obtain a unique identification number. Card holders can have the new application added upon the request of updating. Authentication through the shared common security module can be considered as secure because the new application should always conform to the standard specification from the respective authority which specified the level of security the system is going to achieve. After the application is added, the corresponding service index file should be updated as well.

4.6 Examples and Summary

All the different identification cards and licences issued from the government, such as citizen identification card, driving licence, fishing or hunting license, passport, council's library card, and etc, can be integrated together under the system discussed here, because they all conform to a single specification from the government and act as identification purposes. Another example is the multiple merchant incentives which allow card holders to store "points" for frequent purchaser programs across multiple merchants. This is workable as most of those programs require only basic information of the card holder and lower level of security, therefore those information can be shared together in order to verify the owner. In summary, applications integrated together under this scheme can reduce the repetitive of resources and facilitate the management of different applications.

5. Multiple Independent Applications In A Single Card

The major trend of the next generation smart card is the mergence of multiple independent applications into a single card which enables card holder to accomplish different unrelated tasks with more ease and convenience. This kind of multiple application smart card is always referred as electronic purse or wallet. Figure 8 presents this model.

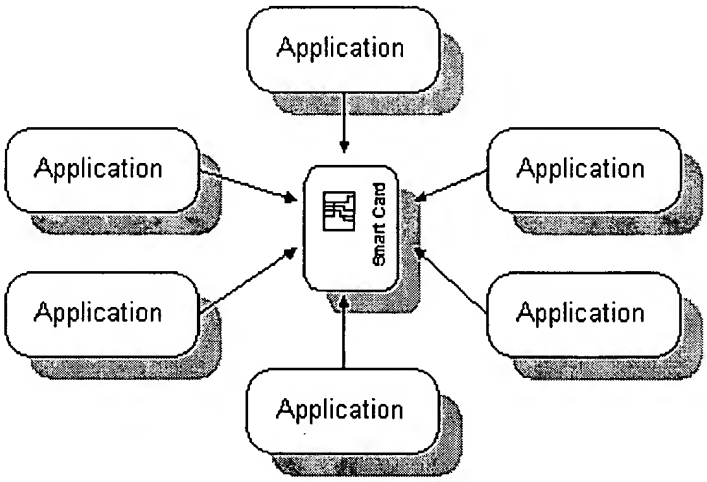

Figure 8: Multiple independent applications in a single smart card

However, in order to build this kind of multiple application smart card, which has to be sophisticated and generic enough to accommodate different kinds of applications without transgressing any existing applications or weakening any existing security mechanisms, we need to break through a lot of different barriers which have always been a source of controversy.

In this section, we try to propose a feasible model in the terms of data ownership and management, directory configuration and partitioning, security and data sharing, application invocation and authentication, etc. However, before we carry on to discuss those issues, we are assumed that there is a standard smart card operating system and a standard specification to specify how applications operate and interface with each others and the outside world.

5.1 Data Ownership and Management

Ownership of the card or data should not be the application provider as a single card contains more than one applications. Card provider claims to be the owner is also impractical as there may not a relationship between the card provider and application providers. Therefore it is recommended the card holder to be the owner. Whenever a person who wants to have services from application providers, he or she can purchase a smart card from one of the card providers and have the application added on it.

The smart card provider can be an agency of different application providers, so that customers can have applications installed on the card when they purchase it. This kind of scheme can be achieved by having an agency which is similar to the post offices in Australia where they are agencies of different organisation such as banks, telecom company, and electricity board, etc.

Management and maintenance of the applications on the card can be done by the card provider as they are authorised by different application providers. For the concerns of security, it will be discussed in the following section.

5.2 Data Directory Configuration and Partitioning

As there is not a central authority to organise and assign identification numbers for applications, duplicated file Id may be used by different applications. Therefore, it is proposed to assign file Ids to applications sequentially and maintained by an index file. When there is a new application, it will be allocated to the next available file Id. The index file would be accessible by anyone without protection, this should not cause the system to become unsecured since there is not any identity or authentication information inside the file. Figure 9 shows an overview of the file structure.

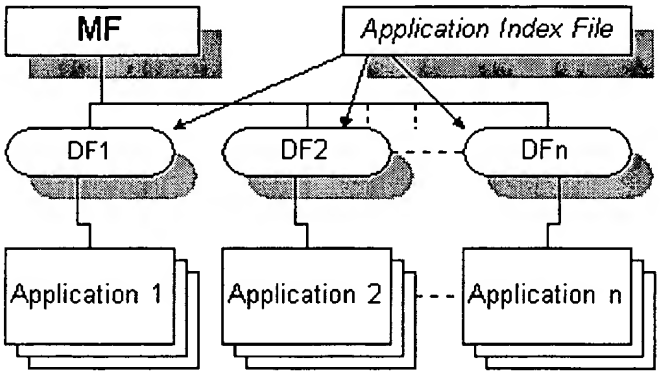

Figure 9: File structure overview

5.3 Security and Data Sharing

It is likely that each embedded applications will have their specific security requirements, so it is difficult to design a multi-application smart card that allows applications sharing the hardware and operating system but keeping different security schemes for individuals. Nevertheless, there is a scheme proposed by Professor Vincent Cordonnier and Anthony Watson in one of their paper called "The concept of suspicion: a new security tool for multi-application smart cards" at 1996 which can fulfil the requirements from various applications. We are going to adapt that scheme and it is described below.

An unique identification module will be created and make available for each existing or future applications. It must be flexible enough to fit with any security policies and to drive any biometric processes. It will supervise various biometric tools and directly communicate with them. This module will act as a component of the card operating system. Figure 10 shows a conceptual view of it.

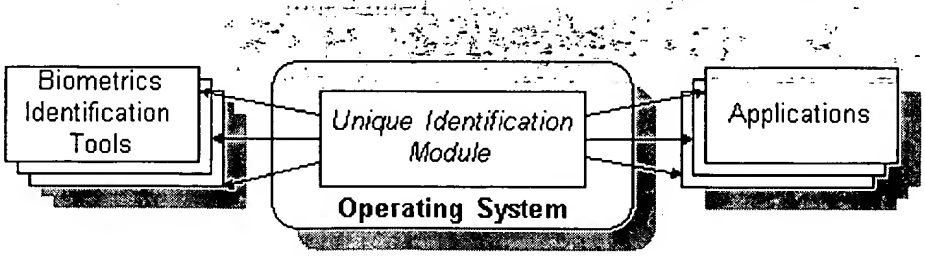

Figure 10: Conceptual view of the security module (source: Cordonnier & Watson, 1996)

According to the application requirements, the identification module can activate one of the available biometric modules. A response will be received from the dedicated biometric module. As different applications may require a more flexible decision process, it is assumed that the result is a standardised number which representing the measurement of the level of matching.

The use of biometric identification here is because it seems to provide a promising result as it uses basic characteristics of the individual and does not require any artificial link between the card holder. Consequently, applications can assign its dedicated identification scheme and the matching level for acceptance, so that the same measurement can lead one application to accept the transaction and the another one refuse.

For the communication and data sharing between each applications, it is required each of them to activate their own identification process. If the result leads one of the application not to be initiated, other applications must receive an alarm. This common evaluation of the risk by all the applications can be implemented by creating a common index of confidence.

For the details of the scheme described above, please refer to the references of Cordonnier & Watson, 1996.

5.4 Application Invocation and Authentication

Applications can be accessed through the index file. However, a search on the file is required in order to select a correct application. Authentication can be made by installing a digital signature scheme on the card, and made use of public and private cryptographic algorithm to protect the access of index file. For the authentication of using applications, the proposed scheme which described in section 5.3 will be used.

5.5 Application Expansion

Apart from the memory size of the smart card, application expansion is not limited under this system. Whenever application providers create new applications which conformed with the standard smart card application programming interface (API), they can distribute their products through the smart card provider or agency.

5.6 Examples and Summary

Multiple application smart card which referenced as electronic wallet by the card industry can adapt or integrate a wide range of applications. It can be a credit or debit card, citizen identification card, driver's license, gas card, and student card, etc. In summary, for a truly multiple application smart card, there should not a limit on what kind of applications are installed on it while the security inside the card is maintained.

6. Conclusion

In this paper, three different kinds of scheme to organise and access of multiple application smart card are discussed. The first and second schemes are practical and workable on these days, and there is real applications developed using those models. For the third one, multiple independent applications in a

single card, there is still a long way to go to make it becomes feasible because of several reasons.

Firstly, consumer education is not enough. It is time consuming and costly to teach consumer to feel comfortable using the smart card for payment instead of using coins or notes for example. It is also necessary to educate card holders to have a sense of security issues as the smart card may contains sensitive and confidential data about themselves such as their medical histories or biometrics information.

Secondly, in the terms of how an operating system should look like, how the applications interface with each other, or what kind of structure or format the data should be, there is not an international standard specification available for the smart card. It is believed that the time to standardise all of these and make all the cards and terminals interchangeable will take much longer than the standardisation of magnetic stripe card which had been done for so many years.

Lastly, with the concerns of personal privacy and security, no matter how the manufacturers claim how their systems are secured and protected, it is difficult to expect consumers to believe that the information they might supply for the purpose of initialising or loading into their smart cards would remain private forever. With the technology today, whenever there is a mechanism to encrypt and protect the data, there is always a way to break the cryptographic algorithm. Therefore, there is always a lot of debates and arguments about the issues in the topics of security.

In conclusion, even though there is a lot of problems ahead, "when all the dust is settled, it is expected that smart cards will be well accepted and as ubiquitous as magnetic stripe cards are today, but with vastly greater capabilities" *(Seidman, 1996)*. Smart cards are the keys to the media and information revolution no matter whether it is wired or wireless.

---

7. References

- Cordonnier & Cordoonier, V. & Watson, A., 1996, *The concept of suspicion: A new security tool*
- Watson, 1996 *for multi-application smart cards*, Recherche et Developpement sur le Dossier Portable, The Universite des Sciences et Technologies de Lille. And School of Mathematics, Information Technology and Engineering, Edith Cowan University.
- Looi, 1995 Looi, M.H., 1995, *Authentication for applications in computer network environments using intelligent tokens*, School of Data Communications. Queensland University of Technology.
- Matilla, 1992 Matilla, P., 1992, *Setec Oy Supplying Multiservice Application and Medical Trial*, Report on Smart Card, April 1992, pp7.
- Seidman, 1996 Seidman, S., 1996, *Emerging markets, persistent problems: Smart cards have come a long way, but still have a long way to go*, Report on Smart Cards, Dec. 1996, pp 3-5.
- Unknow Author 3-G International, Inc., 1997, *Multi-Function Cards*, Internet WWW page at URL: <http://www.3gi.com/sc/sc_multi.htm> (7 May 1997)
- Unknow Author IC One, 1997, *Test of "Electronic Wallet" Undertaken by IC One and State Agencies*, Internet WWW page at URL: <http://www.icone.com/iocp.htm> (9 May 1997)

- Unknow Author Ideas International, 1997, *AFIM to be used for Multiple Applications Smart Card*, Internet WWW page at URL: <http://www.parlant.com/ideas/icone.htm> (7 May 1997)

- Unknow Author NewsPage from individual, 1997, *Gemplus' GemXplore Family of SIM Cards Now Compatible With GSM Phase 2+ Standard*, Internet WWW page at URL: <http://www.newspage.com/NEWSPAGE/info/d7/d3/d1/public.pre/public/A.b0501130.002.bsw27 (7 May 1997)

to my homepage

Email charleschan98@yahoo.com